REMARKS

Claims 1-21 were pending. Claims 6-21 are cancelled without prejudice or disclaimer. Hence, claims 1-5 are pending in the application.

Applicants cancelled claims 6-21 so as to prosecute all method claims in one patent application. Applicants are not conceding in this application that cancelled claims 6-21 are not patentable over the art cited by the Examiner. Claims 6-21 were cancelled solely to facilitate expeditious prosecution of the remaining method claims (claims 1-5). Applicants respectfully reserve the right to pursue these (claims 6-21) and other claims in one or more continuation patent applications.

Claims 1-11, 18-19 and 21 are rejected under 35 U.S.C. §102(e). Claims 12-17 and 20 are rejected under 35 U.S.C. §103(a). Applicants address these rejections below in connection with pending claims 1-5.

I. REJECTIONS UNDER 35 U.S.C. §102(e):

The Examiner has rejected claims 1-5 under 35 U.S.C. §102(e) as being anticipated by Shanklin et al. (U.S. Patent No. 6,578,147) (hereinafter "Shanklin"). Applicants respectfully traverse these rejections for at least the reasons stated below and respectfully request the Examiner to reconsider and withdraw these rejections.

For a claim to be anticipated under 35 U.S.C. §102, each and every claim limitation must be found within the cited prior art reference and arranged as required by the claim. M.P.E.P. §2131.

Applicants respectfully assert that Shanklin does not disclose "coupling selected data from the network data to a parallel pattern detection engine (PPDE), for comparing the selected data in parallel to M sequences of pattern data stored in the PPDE and generating a match output signal when at least one of the M sequences of pattern data compares to a portion of the selected data" as recited in claim 1. The Examiner cites column 2, line 59 – column 3, line 3 of Shanklin as disclosing the above-cited claim limitation. Office Action (11/9/2007), page 3. Applicants respectfully traverse.

Shanklin instead discloses providing multiple sensors at either the output of a router or inside a switch. Column 2, lines 60-62. Shanklin further discloses that each sensor is identical to the other sensors and is capable of performing the same intrusion detection processing. Column 2, lines 62-64. Additionally, Shanklin discloses that the sensors operate in parallel, and analyze packets to determine if any packet or series of packets has a "signature" that matches one of a collection of known intrusion signatures. Column 2, lines 64-67.

Hence, Shanklin discloses having sensors, operating in parallel, to analyze packets to determine if any packet or series of packets has a signature that matches a known intrusion signature.

There is no language in the cited passage that discloses coupling selected data from the network data to a parallel pattern detection engine (PPDE). Neither is there any language in the cited passage that discloses coupling selected data from the network data to a parallel pattern detection engine (PPDE), for comparing the selected data in parallel to M sequences of pattern data stored in the PPDE. Neither is there any language in the cited passage that discloses generating a match output signal when at least one of the M sequences of pattern data compares to a portion of the selected data. Instead, as discussed above, Shanklin discloses having sensors, operating in parallel, to analyze packets to determine if any packet or series of packets has a signature that matches a known intrusion signature. The Examiner has not provided any rational as to how the teaching of having sensors, operating in parallel, to analyze packets to determine if any packet or series of packets has a signature that matches a known intrusion signature necessarily results in the teaching of the above-identified claim limitations. Thus, Shanklin does not disclose all of the limitations of claim 1, and thus Shanklin does not anticipate claim 1. M.P.E.P. §2131.

In response to Applicants' above argument, the Examiner additionally cites column 3, lines 59-67; and column 4, line 44 – column 5, line 11 of Shanklin as disclosing the above-cited claim limitation. Office Action (11/9/2007), page 9. Applicants respectfully traverse.

Shanklin instead discloses that signature analysis uses one or more intrusion detection sensors 11, which are installed on a network segment and are transparent to network performance. Column 4, lines 44-46. Shanklin further discloses that a sensor 11 contains a detection engine, which examines each packet incoming to the sensor 11, including its header and payload. Column 4, lines 54-56. Shanklin further discloses that the sensor 11 also analyzes each packet's relationship to adjacent and related packets in the data stream. Column 4, lines 56-58. Additionally, Shanklin discloses that if the analysis indicates misuse, the sensor may act autonomously to take action, such as disconnection, or it may send an alarm to a separate intrusion detection management station. Column 4, lines 58-61.

Hence, Shanklin discloses a sensor that analyzes each incoming packet, including analyzing each packet's relationship to adjacent and related packets in the data stream. Shanklin further discloses that if the analysis indicates misuse, the sensor may act autonomously to take action, such as disconnection, or it may send an alarm to a separate intrusion detection management station.

There is no language in the cited passage that discloses coupling selected data from the network data to a parallel pattern detection engine (PPDE). Neither is there any language in the cited passage that discloses coupling selected data from the network data to a parallel pattern detection engine (PPDE), for comparing the selected data in parallel to M sequences of pattern data stored in the PPDE. Neither is there any language in the cited passage that discloses generating a match output signal when at least one of the M sequences of pattern data compares to a portion of the selected data. Thus, Shanklin does not disclose all of the limitations of claim 1, and thus Shanklin does not anticipate claim 1. M.P.E.P. §2131.

The Examiner appears to be ignoring claim language. How does the teaching of a sensor analyzing each incoming packet necessarily result in the teaching of coupling selected data from the network data to a parallel pattern detection engine? How does the teaching of a sensor analyzing each incoming packet necessarily result in the teaching of coupling selected data from the network data to a parallel pattern detection engine (PPDE), for comparing the selected data in parallel to M sequences of pattern data stored in the PPDE? Further, how does the teaching of a sensor analyzing each incoming packet necessarily result in the teaching of generating a match output signal when at least one of the M sequences of pattern data compares to a portion of the selected data? The Examiner must provide a basis in fact and/or technical reasoning to support such conclusions. *Ex parte Levy*, 17 U.S.P.Q.2d 1461, 1464 (Bd. Pat. App. & Inter. 1990). That is, the Examiner must provide extrinsic evidence that must make clear that the teaching of a sensor analyzing each incoming packet necessarily results in the teaching of the above-cited claim limitations, and that it would be so recognized by persons of ordinary skill. *In re Robertson*, 169 F.3d 743, 745 (Fed. Cir. 1999). Since the Examiner has not provided any such objective evidence, the Examiner has not presented a *prima facie* case of anticipation for rejecting claim 1. M.P.E.P. §2112.

Claims 2-5 each recite combinations of features of independent claim 1, and hence claims 2-5 are not anticipated by Shanklin for at least the above-stated reasons that claim 1 is not anticipated by Shanklin.

Claims 2-5 recite additional features, which, in combination with the features of the claims upon which they depend, are not anticipated by Shanklin.

For example, Shanklin does not disclose "storing N intrusion signatures in the M PUs sequences of pattern data with corresponding identification (ID) data used to identify which of the N intrusion signatures is detected" as recited in claim 2. The Examiner cites column 6, lines 25-46 of Shanklin as disclosing the above-cited claim limitation. Office Action (11/9/2007), page 3. Applicants respectfully traverse.

Shanklin instead discloses that "for a software implementation of the load balancing unit 22a or 32a, routing to sensors 21 and 31 can be performed with appropriate modifications to existing router software. Column 6, lines 29-31. Shanklin further discloses that like other IP routing, the decision of which sensor 21 or 31 will receive a particular packet (or session of packets) is determined by an address associated with the sensor. Column 6, lines 32-34. Furthermore, Shanklin discloses that for example, each sensor 21 or 31 might have a unique IP address so that routing is performed as with other IP-addressed destinations. Column 6, lines 34-37.

Hence, Shanklin discloses determining which sensor will process a particular packet based on the address associated with the sensor.

There is no language in the cited passage that discloses storing N intrusion signatures in the M PUs sequences of pattern data. Neither is there any language in the cited passage that discloses storing N intrusion signatures in the M PUs sequences of pattern data with corresponding identification (ID) data. Neither is there any language in the cited passage that discloses storing N intrusion signatures in the M PUs sequences of pattern data with corresponding identification (ID) data used to identify which of the N intrusion signatures is detected. Thus, Shanklin does not disclose all of the limitations of claim 2, and thus Shanklin does not anticipate claim 2. M.P.E.P. §2131.

In response to Applicants' above argument, the Examiner additionally cites column 3, lines 59-67; and column 4, line 44 – column 5, line 11 of Shanklin as disclosing the above-cited claim limitation. Office Action (11/9/2007), page 10. Applicants respectfully traverse.

Shanklin instead discloses that signature analysis uses one or more intrusion detection sensors 11, which are installed on a network segment and are transparent to network performance. Column 4, lines 44-46. Shanklin further discloses that a sensor 11 contains a detection engine, which examines each packet incoming to the sensor 11, including its header and payload. Column 4, lines 54-56. Shanklin further discloses that the sensor 11 also analyzes each packet's relationship to adjacent and related packets in the data stream. Column 4, lines 56-58. Additionally, Shanklin discloses that if the analysis indicates misuse, the sensor may act autonomously to take action, such as disconnection, or it may send an alarm to a separate intrusion detection management station. Column 4, lines 58-61.

Hence, Shanklin discloses a sensor that analyzes each incoming packet, including analyzing each packet's relationship to adjacent and related packets in the data stream. Shanklin further discloses that if the analysis indicates misuse, the sensor may act autonomously to take action, such as disconnection, or it may send an alarm to a separate intrusion detection management station.

There is no language in the cited passage that discloses storing N intrusion signatures in the M PUs sequences of pattern data. Neither is there any language in the cited passage that discloses storing N intrusion signatures in the M PUs sequences of pattern data with corresponding identification (ID) data. Neither is there any language in the cited passage that discloses storing N intrusion signatures in the M PUs sequences of pattern data with corresponding identification (ID) data used to identify which of the N intrusion signatures is detected. Thus, Shanklin does not disclose all of the limitations of claim 2, and thus Shanklin does not anticipate claim 2. M.P.E.P. §2131.

The Examiner appears to be ignoring claim language. How does the teaching of a sensor analyzing each incoming packet necessarily result in the teaching of storing N intrusion signatures in the M PUs sequences of pattern data? How does the teaching of a sensor analyzing each incoming packet necessarily result in the teaching of storing N intrusion signatures in the M PUs sequences of pattern data with corresponding identification (ID) data? Further, how does the teaching of a sensor analyzing each incoming packet necessarily result in the teaching of storing N intrusion signatures in the M PUs sequences of pattern data with corresponding identification (ID) data used to identify which of the N intrusion signatures is detected? The Examiner must provide a basis in fact and/or technical reasoning to support such conclusions. *Ex parte Levy*, 17 U.S.P.Q.2d 1461, 1464 (Bd. Pat. App. & Inter. 1990). That is, the Examiner must provide extrinsic evidence that must make clear that the teaching of a sensor analyzing each incoming packet necessarily results in the teaching of the above-cited claim limitations, and that it would be so recognized by persons of ordinary skill. *In re Robertson*, 169 F.3d 743, 745 (Fed. Cir. 1999). Since the Examiner has not provided any such objective evidence, the Examiner has not presented a *prima facie* case of anticipation for rejecting claim 2. M.P.E.P. §2112.

Applicants further assert that Shanklin does not disclose "storing action code indicating action to take in response to detecting a particular one of the N intrusion signatures" as recited in claim 2. The Examiner cites column 4, lines 54-61 of Shanklin as disclosing the above-cited claim limitation. Office Action (11/9/2007), pages 3-4. Applicants respectfully traverse.

Shanklin instead discloses that a sensor 11 contains a detection engine, which examines each packet incoming to the sensor 11, including its header and payload. Column 4, lines 54-56. Shanklin further discloses that the sensor 11 also analyzes each packet's relationship to adjacent and related packets in the data stream. Column 4, lines 56-58. Additionally, Shanklin discloses that if the analysis indicates misuse, the sensor may act autonomously to take action, such as disconnection, or it may send an alarm to a separate intrusion detection management station. Column 4, lines 58-62.

Hence, Shanklin discloses that a sensor contains a detection engine, which examines each packet incoming to the sensor. Shanklin further discloses analyzing each packet's relationship to adjacent and related packets in the data stream.

There is no language in the cited passage that discloses storing action code indicating action to take in response to detecting a particular one of the N intrusion signatures. Thus, Shanklin does not disclose all of the limitations of claim 2, and thus Shanklin does not anticipate claim 2. M.P.E.P. §2131.

In response to Applicants' above argument, the Examiner additionally cites column 3, lines 59-67; and column 4, line 44 – column 5, line 11 of Shanklin as disclosing the above-cited claim limitation. Office Action (11/9/2007), page 10. Applicants respectfully traverse.

Shanklin instead discloses that signature analysis uses one or more intrusion detection sensors 11, which are installed on a network segment and are transparent to network performance. Column 4, lines 44-46. Shanklin further discloses that a sensor 11 contains a detection engine, which examines each packet incoming to the sensor 11, including its header and payload. Column 4, lines 54-56. Shanklin further discloses that the sensor 11 also analyzes each packet's relationship to adjacent and related packets in the data stream. Column 4, lines 56-58. Additionally, Shanklin discloses that if the analysis indicates misuse, the sensor may act autonomously to take action, such as disconnection, or it may send an alarm to a separate intrusion detection management station. Column 4, lines 58-61.

Hence, Shanklin discloses a sensor that analyzes each incoming packet, including analyzing each packet's relationship to adjacent and related packets in the data stream. Shanklin further discloses that if the analysis indicates misuse, the sensor may act autonomously to take action, such as disconnection, or it may send an alarm to a separate intrusion detection management station.

There is no language in the cited passage that discloses storing action code indicating action to take in response to detecting a particular one of the N intrusion signatures. Thus, Shanklin does not disclose all of the limitations of claim 2, and thus Shanklin does not anticipate claim 2. M.P.E.P. §2131.

The Examiner appears to be ignoring claim language. How does the teaching of a sensor analyzing each incoming packet necessarily result in the teaching of storing action code indicating action to take in response to detecting a particular one of the N intrusion signatures? The Examiner must provide a basis in fact and/or technical reasoning to support such a conclusion. *Ex parte Levy*, 17 U.S.P.Q.2d 1461, 1464 (Bd. Pat. App. & Inter. 1990). That is, the Examiner must provide extrinsic evidence that must make clear that the teaching of a sensor analyzing each incoming packet necessarily results in the teaching of the above-cited claim limitation, and that it would be so recognized by persons of ordinary skill. *In re Robertson*, 169 F.3d 743, 745 (Fed. Cir. 1999). Since the Examiner has not provided any such objective evidence, the Examiner has not presented a *prima facie* case of anticipation for rejecting claim 2. M.P.E.P. §2112.

Applicants further assert that Shanklin does not disclose "comparing the selected data to the store N intrusion signatures and generating, at network data speed, a pattern compare signal and particular ID data when a particular one of the N intrusion signatures is detected" as recited in claim 3. The Examiner cites column 2, line 59 – column 3, line 3 of Shanklin as disclosing the above-cited claim limitation. Office Action (11/9/2007), page 4. Applicants respectfully traverse.

Shanklin instead discloses providing multiple sensors at either the output of a router or inside a switch. Column 2, lines 60-62. Shanklin further discloses that each sensor is identical to the other sensors and is capable of performing the same intrusion detection processing. Column 2, lines 62-64. Additionally, Shanklin discloses that the sensors operate in parallel, and analyze packets to determine if any packet or series of packets has a "signature" that matches one of a collection of known intrusion signatures. Column 2, lines 64-67.

Hence, Shanklin discloses having sensors, operating in parallel, to analyze packets to determine if any packet or series of packets has a signature that matches a known intrusion signature.

There is no language in the cited passage that discloses comparing the selected data to the store N intrusion signatures. Neither is there any language in the cited passage that discloses generating, at network data speed, a pattern compare signal and particular ID data. Neither is there any language in the cited passage that discloses generating, at network data speed, a pattern compare signal and particular ID data when a particular one of the N intrusion signatures is detected. Thus, Shanklin does not disclose all of the limitations of claim 3, and thus Shanklin does not anticipate claim 3. M.P.E.P. §2131.

In response to Applicants' above argument, the Examiner additionally cites column 3, lines 59-67; column 4, line 44 – column 5, line 11; and column 6, lines 9-11 of Shanklin as disclosing the above-cited claim limitation. Office Action (11/9/2007), page 11. Applicants respectfully traverse.

Shanklin instead discloses that signature analysis uses one or more intrusion detection sensors 11, which are installed on a network segment and are transparent to network performance. Column 4, lines 44-46. Shanklin further discloses that a sensor 11 contains a detection engine, which examines each packet incoming to the sensor 11, including its header and payload. Column 4, lines 54-56. Shanklin further discloses that the sensor 11 also analyzes each packet's relationship to adjacent and related packets in the data stream. Column 4, lines 56-58. Additionally, Shanklin discloses that if the analysis indicates misuse, the sensor may act autonomously to take action, such as disconnection, or it may send an alarm to a separate intrusion detection management station. Column 4, lines 58-61. Shanklin further discloses that system 30 has a session analyzer 36, which stores information used to detect signatures from different packets in the same session. Column 6, lines 9-11.

Hence, Shanklin discloses a sensor that analyzes each incoming packet, including analyzing each packet's relationship to adjacent and related packets in the data stream. Shanklin further discloses that if the analysis indicates misuse, the sensor may act autonomously to take action, such as disconnection, or it may send an alarm to a separate intrusion detection management station. Shanklin additionally discloses a sensor receiving a packet indicating a signature that would be comprised of different packets from the same session.

There is no language in the cited passage that discloses comparing the selected data to the store N intrusion signatures. Neither is there any language in the cited passage that discloses generating, at network data speed, a pattern compare signal and particular ID data. Neither is there any language in the cited passage that discloses generating, at network data speed, a pattern compare signal and particular ID data when a particular one of the N intrusion signatures is detected. Thus, Shanklin does not disclose all of the limitations of claim 3, and thus Shanklin does not anticipate claim 3. M.P.E.P. §2131.

The Examiner appears to be ignoring claim language. How does the teaching of a sensor analyzing each incoming packet necessarily result in the teaching of comparing the selected data to the store N intrusion signatures? How does the teaching of a sensor analyzing each incoming packet necessarily result in the teaching of generating, at network data speed, a pattern compare signal and particular ID data? Further, how does the teaching of a sensor analyzing each incoming packet necessarily result in the teaching of generating, at network data speed, a pattern compare signal and particular ID data when a particular one of the N intrusion signatures is detected? The Examiner must provide a basis in fact and/or technical reasoning to support such conclusions. *Ex parte Levy*, 17 U.S.P.Q.2d 1461, 1464 (Bd. Pat. App. & Inter. 1990). That is, the Examiner must provide extrinsic evidence that must make clear that the teaching of a sensor analyzing each incoming packet necessarily results in the teaching of the above-cited claim limitations, and that it would be so recognized by persons of ordinary skill. *In re Robertson*, 169 F.3d 743, 745 (Fed. Cir. 1999). Since the Examiner has not provided any such objective evidence, the Examiner has not presented a *prima facie* case of anticipation for rejecting claim 3. M.P.E.P. §2112.

Applicants further assert that Shanklin does not disclose "executing the action code corresponding to the particular one of the N intrusion signatures detected" as recited in claim 3. The Examiner cites column 4, lines 54-61 of Shanklin as disclosing the above-cited claim limitation. Office Action (11/9/2007), pages 4-5.

Shanklin instead discloses that a sensor 11 contains a detection engine, which examines each packet incoming to the sensor 11, including its header and payload. Column 4, lines 54-56. Shanklin further discloses that the sensor 11 also analyzes each packet's relationship to adjacent and related packets in the data stream. Column 4, lines 56-58. Additionally, Shanklin discloses that if the analysis indicates misuse, the sensor may act autonomously to take action, such as disconnection, or it may send an alarm to a separate intrusion detection management station. Column 4, lines 58-62.

Hence, Shanklin discloses that a sensor contains a detection engine, which examines each packet incoming to the sensor. Shanklin further discloses analyzing each packet's relationship to adjacent and related packets in the data stream.

There is no language in the cited passage that discloses executing the action code corresponding to the particular one of the N intrusion signatures detected. Thus, Shanklin does not disclose all of the limitations of claim 3, and thus Shanklin does not anticipate claim 3. M.P.E.P. §2131.

In response to Applicants' above argument, the Examiner additionally cites column 3, lines 59-67; column 4, line 44 – column 5, line 11; and column 6, lines 9-

11 of Shanklin as disclosing the above-cited claim limitation. Office Action (11/9/2007), page 12. Applicants respectfully traverse.

Shanklin instead discloses that signature analysis uses one or more intrusion detection sensors 11, which are installed on a network segment and are transparent to network performance. Column 4, lines 44-46. Shanklin further discloses that a sensor 11 contains a detection engine, which examines each packet incoming to the sensor 11, including its header and payload. Column 4, lines 54-56. Shanklin further discloses that the sensor 11 also analyzes each packet's relationship to adjacent and related packets in the data stream. Column 4, lines 56-58. Additionally, Shanklin discloses that if the analysis indicates misuse, the sensor may act autonomously to take action, such as disconnection, or it may send an alarm to a separate intrusion detection management station. Column 4, lines 58-61. Shanklin further discloses that system 30 has a session analyzer 36, which stores information used to detect signatures from different packets in the same session. Column 6, lines 9-11.

Hence, Shanklin discloses a sensor that analyzes each incoming packet, including analyzing each packet's relationship to adjacent and related packets in the data stream. Shanklin further discloses that if the analysis indicates misuse, the sensor may act autonomously to take action, such as disconnection, or it may send an alarm to a separate intrusion detection management station. Shanklin additionally discloses a sensor receiving a packet indicating a signature that would be comprised of different packets from the same session.

There is no language in the cited passage that discloses executing the action code corresponding to the particular one of the N intrusion signatures detected. Thus, Shanklin does not disclose all of the limitations of claim 3, and thus Shanklin does not anticipate claim 3. M.P.E.P. §2131.

The Examiner appears to be ignoring claim language. How does the teaching of a sensor analyzing each incoming packet necessarily result in the teaching of executing the action code corresponding to the particular one of the N intrusion signatures detected? The Examiner must provide a basis in fact and/or technical reasoning to support such a conclusion. *Ex parte Levy*, 17 U.S.P.Q.2d 1461, 1464

(Bd. Pat. App. & Inter. 1990). That is, the Examiner must provide extrinsic evidence that must make clear that the teaching of a sensor analyzing each incoming packet necessarily results in the teaching of the above-cited claim limitation, and that it would be so recognized by persons of ordinary skill. *In re Robertson*, 169 F.3d 743, 745 (Fed. Cir. 1999). Since the Examiner has not provided any such objective evidence, the Examiner has not presented a *prima facie* case of anticipation for rejecting claim 3. M.P.E.P. §2112.

Applicants further assert that Shanklin does not disclose "an input/output (I/O) interface for coupling data into and out of the PPDE" as recited in claim 4. As understood by Applicants, the Examiner cites column 3, lines 59-67; column 4, line 44 – column 5, line 11; and column 6, lines 9-14 of Shanklin as disclosing the above-cited claim limitation. Office Action (11/9/2007), page 12. Applicants respectfully traverse.

Shanklin instead discloses that signature analysis uses one or more intrusion detection sensors 11, which are installed on a network segment and are transparent to network performance. Column 4, lines 44-46. Shanklin further discloses that a sensor 11 contains a detection engine, which examines each packet incoming to the sensor 11, including its header and payload. Column 4, lines 54-56. Shanklin further discloses that the sensor 11 also analyzes each packet's relationship to adjacent and related packets in the data stream. Column 4, lines 56-58. Additionally, Shanklin discloses that if the analysis indicates misuse, the sensor may act autonomously to take action, such as disconnection, or it may send an alarm to a separate intrusion detection management station. Column 4, lines 58-61. Shanklin further discloses that system 30 has a session analyzer 36, which stores information used to detect signatures from different packets in the same session. Column 6, lines 9-11.

Hence, Shanklin discloses a sensor that analyzes each incoming packet, including analyzing each packet's relationship to adjacent and related packets in the data stream. Shanklin further discloses that if the analysis indicates misuse, the sensor may act autonomously to take action, such as disconnection, or it may send an alarm to a separate intrusion detection management station. Shanklin additionally discloses a sensor receiving a packet indicating a signature that would be comprised of different packets from the same session.

There is no language in the cited passage that discloses an input/output (I/O) interface for coupling data into and out of the PPDE. Thus, Shanklin does not disclose all of the limitations of claim 4, and thus Shanklin does not anticipate claim 4. M.P.E.P. §2131.

Applicants further assert that Shanklin does not disclose "M processing units (PUs), each of the M PUs having compare circuitry for comparing each of the sequence of input data to pattern data stored in each of the M PUs and generating a compare output, wherein an address pointer selecting the pattern data in each of the M PUs is modified in response to a logic state of the compare output and an operation code stored with the pattern data" as recited in claim 4. The Examiner has not specifically addressed this limitation. The Examiner is reminded that in order to establish a *prima facie* case of anticipation, the Examiner must provide a single prior art reference that expressly or inherently describes each and every element as set forth in the claim. *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 U.S.P.Q.2d 1051, 1053 (Fed. Cir. 1987). Since the Examiner has not addressed this limitation, the Examiner has not established a *prima facie* case of anticipation in rejecting claim 4. M.P.E.P. §2131.

Applicants further assert that Shanklin does not disclose "an input bus for coupling the sequence of input data to each of the M PUs in parallel" as recited in claim 4. The Examiner has not specifically addressed this limitation. The Examiner is reminded that in order to establish a *prima facie* case of anticipation, the Examiner must provide a single prior art reference that expressly or inherently describes each and every element as set forth in the claim. *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 U.S.P.Q.2d 1051, 1053 (Fed. Cir. 1987). Since the Examiner has not addressed this limitation, the Examiner has not established a *prima facie* case of anticipation in rejecting claim 4. M.P.E.P. §2131.

Applicants further assert that Shanklin does not disclose "an output bus coupled to the I/O interface for sending output data to the I/O interface" as recited in claim 4. The Examiner has not specifically addressed this limitation. The Examiner is reminded that in order to establish a *prima facie* case of anticipation, the Examiner must provide a single prior art reference that expressly or inherently describes each and every element as set forth in the claim. *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 U.S.P.Q.2d 1051, 1053 (Fed. Cir. 1987). Since the Examiner has not addressed this limitation, the Examiner has not established a *prima facie* case of anticipation in rejecting claim 4. M.P.E.P. §2131.

Applicants further assert that Shanklin does not disclose "control circuitry coupled to the I/O interface and coupling control data on a control data bus and identification (ID) on an ID bus to each of the M processing units" as recited in claim 4. The Examiner has not specifically addressed this limitation. The Examiner is reminded that in order to establish a *prima facie* case of anticipation, the Examiner must provide a single prior art reference that expressly or inherently describes each and every element as set forth in the claim. *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 U.S.P.Q.2d 1051, 1053 (Fed. Cir. 1987). Since the Examiner has not addressed this limitation, the Examiner has not established a *prima facie* case of anticipation in rejecting claim 4. M.P.E.P. §2131.

Applicants further assert that Shanklin does not disclose "ID selection circuitry for selecting a match ID from ID data identifying the M PUs in response to a pattern match signal and match mode data, wherein the match ID and match data corresponding to the match ID are saved in a temporary register as the output data" as recited in claim 4. The Examiner cites Figure 4 and column 7, lines 1-27 of Shanklin as disclosing the above-cited claim limitations. Office Action (11/9/2007), page 5. Applicants respectfully traverse.

Shanklin instead discloses that Figure 4 illustrates a switch 40 having internal intrusion detection sensors 41. Column 7, lines 20-21. Shanklin further discloses that switch 40 has multiple ports, each having an associated port adapter 44 and each capable of supporting a single end station or another network. Column 7, lines 21-23. Shanklin additionally discloses that packets are forwarded by switch 40 based on the destination address. Column 7, lines 23-24.

Hence, Shanklin discloses a switch having internal intrusion detection sensors where packets are forwarded by the switch based on the destination address.

There is no language in the cited passage that discloses ID selection circuitry for selecting a match ID from ID data identifying the M PUs. Neither is there any language in the cited passage that discloses ID selection circuitry for selecting a match ID from ID data identifying the M PUs in response to a pattern match signal. Neither is there any language in the cited passage that discloses ID selection circuitry for selecting a match ID from ID data identifying the M PUs in response to a pattern match signal and match mode data. Neither is there any language in the cited passage that discloses ID selection circuitry for selecting a match ID from ID data identifying the M PUs in response to a pattern match signal and match mode data, where the match ID and match data corresponding to the match ID are saved in a temporary register. Neither is there any language in the cited passage that discloses ID selection circuitry for selecting a match ID from ID data identifying the M PUs in response to a pattern match signal and match mode data, where the match ID and match data corresponding to the match ID are saved in a temporary register as the output data. Thus, Shanklin does not disclose all of the limitations of claim 4, and thus Shanklin does not anticipate claim 4. M.P.E.P. §2131.

Applicants further assert that Shanklin does not disclose "wherein the PPDE further comprises cascade circuitry coupled from each of the M PUs to one or more adjacent PUs within the M PUs for selectively coupling chain data between one or more groups of two or more adjacent PUs selected from the M PUs in response to the control data" as recited in claim 5. The Examiner cites Figure 4 and column 4, lines 54-61 of Shanklin as disclosing the above-cited claim limitation. Office Action (11/9/2007), page 6. Applicants respectfully traverse.

Shanklin instead discloses that a sensor 11 contains a detection engine, which examines each packet incoming to the sensor 11, including its header and payload. Column 4, lines 54-56. Shanklin further discloses that the sensor 11 also analyzes each packet's relationship to adjacent and related packets in the data stream. Column 4, lines 56-58. Additionally, Shanklin discloses that if the analysis indicates misuse, the sensor may act autonomously to take action, such as disconnection, or it may send an alarm to a separate intrusion detection management station. Column 4, lines 58-62.

Hence, Shanklin discloses that a sensor contains a detection engine, which examines each packet incoming to the sensor. Shanklin further discloses analyzing each packet's relationship to adjacent and related packets in the data stream.

There is no language in the cited passage that discloses that the PPDE further comprises cascade circuitry coupled from each of the M PUs to one or more adjacent PUs within the M PUs. Neither is there any language in the cited passage that discloses that the PPDE further comprises cascade circuitry coupled from each of the M PUs to one or more adjacent PUs within the M PUs for selectively coupling chain data between one or more groups of two or more adjacent PUs selected from the M PUs. Neither is there any language in the cited passage that discloses that the PPDE further comprises cascade circuitry coupled from each of the M PUs to one or more adjacent PUs within the M PUs for selectively coupling chain data between one or more groups of two or more adjacent PUs selected from the M PUs in response to the control data. Thus, Shanklin does not disclose all of the limitations of claim 5, and thus Shanklin does not anticipate claim 5. M.P.E.P. §2131.

In response to Applicants' above argument, the Examiner additionally cites column 3, lines 59-67; column 4, line 44 – column 5, line 11; column 6, lines 9-14 and 25-46; and column 7, lines 53-59 of Shanklin as disclosing the above-cited claim limitation. Office Action (11/9/2007), page 12. Applicants respectfully traverse.

Shanklin instead discloses that signature analysis uses one or more intrusion detection sensors 11, which are installed on a network segment and are transparent to network performance. Column 4, lines 44-46. Shanklin further discloses that a sensor 11 contains a detection engine, which examines each packet incoming to the sensor 11, including its header and payload. Column 4, lines 54-56. Shanklin further discloses that the sensor 11 also analyzes each packet's relationship to adjacent and related packets in the data stream. Column 4, lines 56-58. Additionally, Shanklin discloses that if the analysis indicates misuse, the sensor may act autonomously to take action, such as disconnection, or it may send an alarm to a separate intrusion detection management station. Column 4, lines 58-61. Shanklin further discloses that system 30 has a session analyzer 36, which stores information used to detect signatures from different packets in the same session. Column 6, lines 9-11. In addition, Shanklin discloses that load balancer 42 provides "session-based" load balancing, where all packets for a particular session are delivered to the same one of sensors 31. Column 7, lines 54-57. In particular, Shanklin discloses that load balancer 42 operates by inspecting each packet of the entire stream of network traffic and retransmitting them to the appropriate sensor 41. Column 7, lines 57-59.

Hence, Shanklin discloses a sensor that analyzes each incoming packet, including analyzing each packet's relationship to adjacent and related packets in the data stream. Shanklin further discloses that if the analysis indicates misuse, the sensor may act autonomously to take action, such as disconnection, or it may send an alarm to a separate intrusion detection management station. Shanklin additionally discloses a sensor receiving a packet indicating a signature that would be comprised of different packets from the same session. Shanklin further discloses "session-based" load balancing, where all packets for a particular session are delivered to the same one of sensors.

The Examiner asserts that these cited passages teach that the IDS sensors are configured in a series that are adjacent to one another and further data can be load balanced between sensors by encapsulating incoming packets. Office Action (11/9/2007), page 13. Applicants could not identify any language in the cited passages to support the assertion that IDS sensors are configured in a series and that data can be load balanced between sensors by encapsulating incoming packets. Applicants respectfully request the Examiner to particularly point out in Shanklin where Shanklin discloses these concepts pursuant to 37 C.F.R. §1.104(c)(2).

Further, there is no language in the cited passages that discloses that the PPDE further comprises cascade circuitry coupled from each of the M PUs to one or more adjacent PUs within the M PUs. Neither is there any language in the cited passages that discloses that the PPDE further comprises cascade circuitry coupled from each of the M PUs to one or more adjacent PUs within the M PUs for selectively coupling chain data between one or more groups of two or more adjacent PUs selected from the M PUs. Neither is there any language in the cited passages that discloses that the PPDE further comprises cascade circuitry coupled from each of the M PUs to one or more adjacent PUs within the M PUs for selectively coupling chain data between one or more groups of two or more adjacent PUs selected from the M PUs in response to the control data. Thus, Shanklin does not disclose all of the limitations of claim 5, and thus Shanklin does not anticipate claim 5. M.P.E.P. §2131.

As a result of the foregoing, Applicants respectfully assert that not each and every claim limitation was found within Shanklin, and thus claims 1-5 are not anticipated by Shanklin. M.P.E.P. §2131.

II. CONCLUSION:

As a result of the foregoing, it is asserted by Applicants that claims 1-5 in the Application are in condition for allowance, and Applicants respectfully request an allowance of such claims. Applicants respectfully request that the Examiner call Applicants' attorney at the below listed number if the Examiner believes that such a discussion would be helpful in resolving any remaining issues.

Respectfully submitted,

WINSTEAD P.C.

Attorneys for Applicants

By:____________________
Robert A. Voigt, Jr.
Reg. No. 47,159

P.O. Box 50784
Dallas, TX 75201
(512) 370-2832